DUMPS BASE

EXAM DUMPS

ISTQB CT-SEC

28% OFF Automatically For You

ISTQB Certified Tester Security Tester (CT-SEC)

1.What is the primary goal of security testing?
A. To find all possible defects in the software
B. To ensure the software meets all functional requirements
C. To identify vulnerabilities and weaknesses in the system
D. To improve the user interface design
Answer: C

2.What is the difference between authentication and authorization in security testing?
A. Authentication focuses on identifying the user, while authorization determines what the user can access
B. Authentication and authorization are the same thing
C. Authentication ensures data encryption, while authorization verifies user credentials
D. Authentication is not relevant to security testing
Answer: A

3.Why is it important to consider threat modeling in security testing?
A. Threat modeling helps prioritize security vulnerabilities based on risk
B. Threat modeling is not relevant to security testing
C. Threat modeling only applies to physical security, not software security
D. Threat modeling is a one-time activity and does not need to be revisited
Answer: A

4.What is the purpose of a security risk assessment in security testing?
A. To ensure the software meets all functional requirements
B. To identify security vulnerabilities and potential impacts on the system
C. To test the performance of the software under high load conditions
D. To validate user interface design
Answer: B

5.Why is it important to understand the security requirements of a system before conducting security testing?
A. Understanding security requirements helps prioritize security testing efforts
B. Security requirements have no impact on security testing
C. Security requirements are only relevant for compliance purposes
D. Understanding security requirements is not necessary for security testing
Answer: A

ISTQB CT-SEC Dumps (v8.02) with Real Question and Answers - Pass Your Exam

6.What is the primary purpose of security testing in software development?
A. Ensuring the functionality of the software
B. Ensuring the scalability of the software
C. Ensuring the security of the software
D. Ensuring the efficiency of the software
Answer: C

7.What is the goal of security testing?
A. To identify functional bugs
B. To verify the user interface design
C. To uncover security vulnerabilities
D. To enhance software performance
Answer: C

8.Which of the following is a common strategy used in security testing?
A. Black-box testing only
B. White-box testing only
C. Grey-box testing
D. Usability testing
Answer: C

9.When should security testing be conducted in the software development lifecycle?
A. Only in the testing phase
B. After the software is deployed
C. Throughout the software development lifecycle
D. At the end of the project
Answer: C

ISTQB CT-SEC Dumps (V8.02) with Real Questions and Answers - Pass Your Exam

10.What is a key strategy in ensuring the success of security testing?
A. Use of outdated security tools
B. Regularly updating security mechanisms
C. Ignoring security best practices
D. Skipping security evaluation and reporting
Answer: B

11.What is the first step in the security testing process?
A. Identify security vulnerabilities
B. Define security testing objectives

C. Analyze security risks
D. Develop a security testing plan
Answer: B

12.Which of the following is NOT a common approach to security testing processes?
A. White-box testing
B. Black-box testing
C. Spider testing
D. Gray-box testing
Answer: C

13.During the security testing process, what does the term "penetration testing" refer to?
A. Testing the application for security vulnerabilities
B. Testing the application from a user perspective
C. Using automated tools to test security mechanisms
D. Simulating a real-world attack on the application
Answer: D

14.Which phase of the security testing process involves scanning the application for known security vulnerabilities?
A. Planning
B. Execution
C. Analysis
D. Reporting
Answer: B

ISTQB CT-SEC Dumps (V8.02) with Real Questions and Answers - Pass Your Exam

15.What is the purpose of a security testing report?
A. To detail the steps taken during the security testing process
B. To report on the findings of security testing activities
C. To provide recommendations for security enhancements
D. To outline the security testing strategy
Answer: B

16.When should security testing ideally begin in the software development lifecycle?
A. During design phase
B. During development phase
C. During testing phase

D. During deployment phase
Answer: A

17.What is the purpose of conducting security testing during the maintenance phase of the software lifecycle?
A. To identify security vulnerabilities
B. To implement security controls
C. To monitor security incidents
D. To update security documentation
Answer: C

18.Which security testing technique is commonly used during the requirements gathering phase of the software lifecycle?
A. Penetration testing
B. Risk assessment
C. Security code review
D. Security requirements analysis
Answer: D

19.What is the primary goal of security testing during the deployment phase of the software lifecycle?
A. To ensure data encryption
B. To assess software performance
C. To detect security flaws
D. To validate access controls
Answer: C

ISTQB CT-SEC Dumps (V8.02) with Real Questions and Answers - Pass Your Exam

20.Which of the following activities is not part of the security testing process during the maintenance phase?
A. Security patch management
B. Incident response planning
C. Regular security training for developers
D. Initial security risk assessment
Answer: D

21.Which of the following security mechanisms is used to encrypt data in transit?
A. SSL/TLS
B. Firewall

C. Intrusion Detection System
D. Antivirus
Answer: A

22.What type of security mechanism is used to prevent unauthorized access to a network?
A. Two-factor authentication
B. Access control lists
C. Encryption
D. Vulnerability scanning
Answer: B

23.Which security mechanism is used to identify and manage software vulnerabilities?
A. Penetration Testing
B. Intrusion Detection System
C. Antivirus
D. Vulnerability scanning
Answer: D

24.Which security mechanism is used to protect against malicious software?
A. Intrusion Prevention System
B. Antivirus
C. Data Loss Prevention
D. Two-factor authentication
Answer: B

25.Which security mechanism helps to monitor and analyze network traffic for potential security threats?
A. Web Application Firewall
B. Intrusion Detection System
C. Encryption
D. Penetration Testing
Answer: B

26.When conducting security testing, why is it important to consider the human factor in addition to technical aspects?
A. Humans are not a significant factor in security testing

ISTQB CT-SEC Dumps (V8.02) with Real Questions and Answers - Pass Your Exam

B. Human errors can lead to security vulnerabilities
C. Humans have no influence on the effectiveness of security controls
D. Human behavior has no impact on security risks
Answer: B

27.Which of the following is an example of a human factor that can affect security testing?
A. Lack of training for testers
B. Use of complex algorithms in testing tools
C. High network traffic during testing
D. Excessive use of automation in testing
Answer: A

28.How can social engineering play a role in security testing?
A. Social engineering is not relevant to security testing
B. Social engineering can be used to exploit human vulnerabilities
C. Social engineering only affects technical aspects of security
D. Social engineering is a type of security testing tool
Answer: B

29.In security testing, why is it important to consider the psychology of users?
A. User psychology has no impact on security testing
B. Understanding user behavior can help identify security risks
C. User psychology does not affect the effectiveness of security controls
D. Users are not a relevant factor in security testing
Answer: B

ISTQB CT-SEC Dumps (v8.02) with Real Questions and Answers - Pass Your Exam

30.How can user awareness training contribute to security testing?
A. User awareness training is not relevant to security testing
B. Training users can help prevent security incidents
C. User training has no impact on the effectiveness of security controls
D. User awareness is only important for developers, not testers
Answer: B

31.What is the purpose of conducting a security test evaluation and reporting?
A. To identify potential vulnerabilities in the system
B. To clear any bugs found during testing
C. To enhance the performance of the software

D. To increase the complexity of security measures
Answer: A

32.Which of the following is NOT a common metric used for evaluating security test results?
A. False positive rate
B. False negative rate
C. Mean time to repair
D. Code coverage
Answer: D

33.What is the significance of documenting detailed results and findings during security testing evaluation?
A. It is unnecessary and adds extra burden on the team
B. It helps in tracking progress and communicating with stakeholders
C. It can lead to a security breach
D. It slows down the testing process
Answer: B

34.When should security test reports be shared with stakeholders?
A. Only after all vulnerabilities have been fixed
B. Only if the test results are positive
C. As soon as they are available
D. Only during formal meetings
Answer: C

35.What should be included in a comprehensive security test report?
A. Only the test results
B. Recommendations for improvements
C. Date and time of testing
D. Only the vulnerabilities identified
Answer: B

36.Which of the following is a popular open-source security testing tool used for scanning web applications for vulnerabilities?
A. Nessus
B. Metasploit
C. Burp Suite

ISTQB CT-SEC Dumps (V8.02) with Real Questions and Answers - Pass Your Exam

D. OWASP ZAP
Answer: D

37.Which type of security testing tool is commonly used for analyzing network traffic and detecting potential intrusions?
A. Static Application Security Testing (SAST) tool
B. Dynamic Application Security Testing (DAST) tool
C. Network Vulnerability Scanner
D. Web Application Firewall (WAF)
Answer: C

38.Which security testing tool is specifically used for fuzz testing, a technique where invalid or unexpected inputs are provided to a system to uncover vulnerabilities?
A. Wireshark
B. Peach Fuzzer
C. Nmap
D. Acunetix
Answer: B

39.Which category of security testing tools focuses on analyzing source code for potential security vulnerabilities?
A. Data Loss Prevention (DLP) tools
B. SAST tools
C. DAST tools
D. Application Performance Monitoring (APM) tools
Answer: B

ISTQB CT-SEC Dumps (V8.02) with Real Questions and Answers - Pass Your Exam

40.Which security testing tool is commonly used for managing and orchestrating security tests across different platforms and environments?
A. Jenkins
B. Selenium
C. Kali Linux
D. AppScan
Answer: A

41.Which of the following standards is focused on information security management systems?
A. ISO 9001

B. ISO/IEC 27001
C. ISO 14001
D. ISO 31000
Answer: B

42.What is one industry trend in security testing?
A. Manual testing is becoming obsolete
B. Automation of security testing is on the rise
C. Security testing is not a priority for organizations
D. Security testing is only focused on network security
Answer: B

43.Which of the following organizations is responsible for developing the OWASP Top 10 list of web application vulnerabilities?
A. NIST
B. ISC2
C. OWASP
D. IEEE
Answer: C

ISTQB CT-SEC Dumps (v8.02) with Real Questions and Answers - Pass Your Exam

44.What is the purpose of following industry standards in security testing?
A. To make the testing process more complicated
B. To ensure compatibility with different software tools
C. To establish a baseline for good security practices
D. To confuse testers with unnecessary requirements
Answer: C

45.Which of the following industry trends emphasizes the importance of incorporating security into the development process from the start?
A. Reactive security measures
B. Shift-left security
C. Manual security testing only
D. Security testing as an afterthought
Answer: B

46.What is the primary objective of security testing in software development?
A. Enhancing user experience
B. Maximizing profitability

C. Identifying vulnerabilities and potential threats
D. Improving code readability
Answer: C

47.Which of the following is NOT a common type of security testing?
A. Penetration testing
B. Load testing
C. Vulnerability assessment
D. Risk assessment
Answer: B

48.What is the difference between security testing and functional testing?
A. Security testing focuses on performance, while functional testing focuses on security.
B. Security testing ensures the confidentiality, integrity, and availability of the system, while functional testing focuses on individual functions of the system.
C. Security testing is only performed in production, while functional testing is performed in development.
D. Security testing does not involve automated tools, while functional testing heavily relies on automation.
Answer: B

ISTQB CT-SEC Dumps (V8.02) with Real Questions and Answers. Pass Your Exam

49.Why is it important for security testing to be integrated into the software development lifecycle?
A. To reduce costs associated with fixing security issues after deployment
B. To conduct regular security audits
C. To ensure the software meets functional requirements
D. To improve user experience
Answer: A

50.What role does risk assessment play in security testing?
A. Risk assessment helps prioritize which security measures should be implemented first.
B. Risk assessment focuses on identifying coding errors in the software.
C. Risk assessment is only relevant for large-scale software projects.
D. Risk assessment is not related to security testing.
Answer: A

51.What is the primary purpose of security testing in a software development lifecycle?
A. To identify and mitigate security vulnerabilities before deployment
B. To ensure the software meets performance requirements
C. To prioritize user experience over security measures
D. To track software usage by end-users
Answer: A

52.Which of the following is a common goal of security testing?
A. To improve the software's user interface
B. To detect and prevent unauthorized access
C. To reduce the cost of software development
D. To increase the number of software features
Answer: B

53.What is one of the strategies used in security testing to enhance the security of a system?
A. Conducting performance testing only
B. Implementing strong authentication mechanisms
C. Skimping on code reviews and analysis
D. Applying minimal security controls
Answer: B

54.What is the end goal of security testing in a software development project?
A. To delay the project release date
B. To increase the complexity of the software code
C. To ensure the confidentiality, integrity, and availability of data
D. To introduce as many security vulnerabilities as possible
Answer: C

55.Which of the following is a common strategy for conducting security testing throughout the software development lifecycle?
A. Only conducting security testing at the end of the project
B. Introducing security testing at each phase of the project
C. Avoiding security testing altogether
D. Only focusing on functional testing
Answer: B

ISTQB CT-SEC Dumps (v8.02) with Real Questions and Answers - Pass Your Exam

56.What is the first step in the security testing process?
A. Identifying security vulnerabilities
B. Planning security tests
C. Documenting security protocols
D. Executing security tests
Answer: B

57.Which of the following is NOT a common security testing technique?
A. Penetration testing
B. Vulnerability scanning
C. Load testing
D. Static code analysis
Answer: C

58.What is the purpose of conducting a security risk assessment?
A. To identify security vulnerabilities
B. To prioritize areas for security testing
C. To classify testing tools
D. To automate security testing processes
Answer: B

59.When conducting security testing, what does a false positive result indicate?
A. A security vulnerability is present
B. No security vulnerabilities are present
C. An incorrect identification of a vulnerability
D. A critical security flaw
Answer: C

ISTQB CT-SEC Dumps (v8.02) with Real Questions and Answers - Pass Your Exam

60.Which phase of the software development lifecycle is ideal for integrating security testing?
A. Testing phase
B. Planning phase
C. Requirements phase
D. Design phase
Answer: D

61.In which phase of the software development lifecycle is security testing typically first introduced?

A. Planning
B. Requirements
C. Design
D. Implementation
Answer: B

62.What is the primary goal of security testing throughout the software lifecycle?
A. To find all bugs in the software
B. To ensure the software is user-friendly
C. To identify and mitigate security risks
D. To improve software performance
Answer: C

63.Which of the following activities is NOT part of security testing throughout the software lifecycle?
A. Threat modeling
B. Penetration testing
C. Code reviews
D. User acceptance testing
Answer: D

64.How can security testing be integrated into the Agile software development lifecycle?
A. By conducting security testing at the end of the project
B. By performing security testing only during the requirements phase
C. By incorporating security testing into each sprint
D. By outsourcing security testing to a third-party vendor
Answer: C

ISTQB CT-SEC Dumps (v8.02) with Real Questions and Answers - Pass Your Exam

65.Why is it important to perform security testing throughout the software lifecycle?
A. To meet regulatory compliance requirements
B. To reduce the likelihood of security breaches
C. To improve software functionality
D. To speed up the software development process
Answer: B

66.What is the primary purpose of penetration testing in security testing?
A. To identify vulnerabilities in a system

B. To encrypt data transmission
C. To monitor user activities
D. To improve user interface design
Answer: A

67.Which of the following is an example of a security mechanism used to protect web applications from cross-site scripting attacks?
A. Firewall
B. Encryption
C. Input validation
D. Authorization controls
Answer: C

68.What is the purpose of using role-based access control (RBAC) in security testing?
A. To monitor network traffic
B. To encrypt data at rest
C. To control access rights based on user roles
D. To back up sensitive data
Answer: C

69.Which of the following security mechanisms can be used to prevent SQL injection attacks?
A. Secure socket layer (SSL)
B. Cross-origin resource sharing (CORS)
C. Input validation
D. Multi-factor authentication
Answer: C

ISTQB CT-SEC Dumps (V8.02) with Real Questions and Answers - Pass Your Exam

70.What is the purpose of using encryption as a security mechanism in software applications?
A. To monitor system performance
B. To authenticate users
C. To secure data transmission
D. To validate input fields
Answer: C

71.When conducting security testing, which human factor is related to the ability to recognize and respond to suspicious activity or security threats?

A. Lack of training
B. Overconfidence
C. Complacency
D. Poor communication
Answer: B

72.Which human factor in security testing pertains to the tendency for individuals to resist change or new security protocols?
A. Complacency
B. Fear of failure
C. Resistance to change
D. Lack of awareness
Answer: C

73.Which human factor involves jeopardizing security through negligent or reckless behavior, such as sharing passwords or leaving sensitive information unattended?
A. Lack of vigilance
B. Lack of motivation
C. Carelessness
D. Inadequate training
Answer: C

74.In the context of security testing, which human factor encompasses employees feeling undervalued or disconnected from security protocols, leading to potential security breaches?
A. Lack of awareness
B. Lack of motivation
C. Lack of trust
D. Lack of accountability
Answer: C

75.Which human factor in security testing refers to the tendency for individuals to prioritize convenience or efficiency over security measures?
A. Lack of motivation
B. Impatience
C. Lack of awareness
D. Complacency
Answer: B

ISTQB CT-SEC Dumps (v8.02) with Real Questions and Answers, Pass Your Exam

76.What is the purpose of security test evaluation and reporting in the security testing process?
A. To identify security vulnerabilities
B. To communicate test results to stakeholders
C. To fix security issues in the software
D. To improve the software development process
Answer: B

77.Which of the following is NOT a common component of a security test report?
A. Test objectives
B. Test plan
C. Test results
D. Test environment details
Answer: D

78.Why is it important to provide recommendations in a security test report?
A. To demonstrate technical expertise
B. To highlight areas for improvement
C. To increase the length of the report
D. To align with industry standards
Answer: B

ISTQB CT-SEC Dumps (v8.02) with Real Questions and Answers - Pass Your Exam

79.How should security test results be documented in a report?
A. With vague descriptions
B. With technical jargon
C. With clear and concise language
D. With lengthy paragraphs
Answer: C

80.Which stakeholders should typically receive a security test report?
A. Only the development team
B. Only the security team
C. Only the management team
D. All relevant stakeholders
Answer: D

GET FULL VERSION OF CT-SEC DUMPS